

UNITED STATES DISTRICT COURT

for the
WESTERN DISTRICT OF OKLAHOMA

In the Matter of the Search of)

(Briefly describe the property to be search)

(Or identify the person by name and address))

INFORMATION ASSOCIATED WITH:)

Dell All-In-One computer, serial number FLQB022;)

Dell Laptop computer, serial number 9R923S1;)

Western Digital hard drive, serial number)

WCC1S7961393; Seagate hard drive, serial number)

W1F4FBQR; Sandisk solid state drive, serial number)

124675402476.)

THAT IS STORED AT PREMISES CONTROLLED BY:)

Currently Located at The Federal Bureau of)

Investigation, Oklahoma City, Oklahoma)

Case No:

M-19-589-P

FILED

NOV -8 2019

CARMELITA REEDER SHIN
CLERK U.S. DISTRICT COURT
BY: Carmelita Reeder Shin
DEPUTYAPPLICATION FOR SEARCH WARRANT

I, a federal law enforcement officer or attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property (*identify the person or describe property to be searched and give its location*):

See Attachment A, which is attached and incorporated by reference.

Located in the Western District of Oklahoma, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment B, which is attached and incorporated by reference.

The basis for the search under Fed. R. Crim.P.41(c) is (*check one or more*):

- ☒ evidence of the crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. § 2252

Offense Description

Access, and attempt to access, with intent to view child pornography

The application is based on these facts:

See attached Affidavit of Special Agent Richard Whisman, Federal Bureau of Investigation, which is incorporated by reference herein.

☒ Continued on the attached sheet(s).

☐ Delayed notice of _____ days (*give exact ending date if more than 30 days*) is requested under 18

U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s).

Richard Whisman
Applicant's signature

RICHARD WHISMAN
Special Agent
Federal Bureau of Investigation

Sworn to before me and signed in my presence.

Date: 11/8/19

City and State: Oklahoma City, Oklahoma

A handwritten signature in black ink, appearing to read "Gary M. Purcell", written over a horizontal line.

Judge's signature

GARY M. PURCELL, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A

Property to Be Searched

The property items to be searched are: a Dell All-In-One computer with serial number FLQB022, a Dell Laptop computer with serial number 9R923S1, a Western Digital hard drive with serial number WCC1S7961393, a Seagate hard drive with serial number W1F4FBQR, and a SanDisk solid state drive with serial number 124675402476, which are currently in the possession of the Federal Bureau of Investigation in Oklahoma City, Oklahoma.

ru
sub

ATTACHMENT B

Particular Things to be seized

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Section 2252, for distributing and accessing, and attempting to access, with intent to view child pornography:

1. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;
 - d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
 - e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
 - f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
 - g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
 - h. evidence of the times the COMPUTER was used;

rw
amb

- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
- m. contextual information necessary to understand the evidence described in this attachment.
- n. Child pornography and child erotica, and evidence of accessing the same.

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

A handwritten signature in black ink, appearing to be 'JW' followed by a stylized flourish.

**THE UNITED STATES DISTRICT COURT FOR THE WESTERN
DISTRICT OF OKLAHOMA**

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Richard Whisman, being first duly sworn, hereby depose and state as follows:

Introduction and Agent Background

I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property, which are electronic devices, currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

1. I am a Special Agent with the Federal Bureau of Investigation, and have been for approximately Seventeen years. I am currently assigned to the Tulsa Resident Agency of the Oklahoma City Division. Prior to becoming a Special Agent with the FBI, I was employed for about seven years as a Police Officer with the West Chicago, Illinois Police Department. Since joining the FBI, I have investigated violations of federal law, to include federal violations concerning computer crimes and child exploitation. I have gained experience through training in classes and work related to conducting these types of investigations. Further, as a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

Identification of the Devices to be Examined

2. The property items to be searched are: a Dell All-In-One computer with serial number FLQB022, a Dell Laptop computer with serial number 9R923S1, a Western Digital hard

drive with serial number WCC1S7961393, a Seagate hard drive with serial number W1F4FBQR, and a SanDisk solid state drive with serial number 124675402476. These items are currently in the possession of the Federal Bureau of Investigation in Oklahoma City, Oklahoma, hereinafter the “Devices.”

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other law enforcement officers and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Section 2252 (access, and attempt to access, with intent to view child pornography) are presently located ON the Devices. There is also probable cause to search the Devices as described in Attachment A for evidence of these crimes as listed in Attachment B.

Background On Computers And Child Pornography

5. Computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To distribute these images on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls.

6. The development of computers has changed this; computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage.

7. Child pornographers can now transfer photographs from a camera onto a computer readable format with a device known as a scanner. With the advent of digital cameras, the images can be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world.

8. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The storage capability of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously over the years. These drives can store hundreds of thousands of images at a very high resolution.

9. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

10. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, Microsoft, and Google, among others. The online services allow a user to set up an account with a remote computing service that provides e mail services as well as electronic storage of computer files in a variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer.

11. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or Internet Service Provider client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner can often recover evidence which shows that a computer contains peer to peer software, when the computer was sharing files, and even some of the files which were uploaded or downloaded. Such information may be maintained indefinitely until overwritten by other data.

12. A popular tool used by individuals involved in the collection and distribution of child pornography on the Internet, is peer to peer file sharing (hereinafter, "P2P"). P2P file sharing is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. P2P software is readily available for download on the Internet and is often available for free. In general, P2P software allows the user to set-up file(s) on his computer so that the files can be shared with others running compatible P2P software. In essence, a user allows his computer to be searched and accessed by other users of the network. If another user finds a file of interest on his computer, the P2P software allows that other user to download the file from your computer. A user obtains files by opening the P2P software on his computer and typing in a search term or terms. The P2P software then conducts a search of all computers connected to that network to determine whether

any files matching the search term are currently being shared by any other user on that network. The P2P software programs known as eMule, Ares Galaxy, LimeWire, FrostWire, and many other types of P2P software, sets up its searches by keywords. The results of a keyword search are displayed to the user. The user then selects file(s) from the results for download. The download of a file is achieved through a direct connection between the computer requesting the file and one or more computers on the same network containing the file.

13. The strength of the P2P Networks is that they base all of their file shares on a hashing algorithm. Hashing uses mathematical algorithms which allows for the creation of an alpha-numeric value specific and unique to that file, which is the equivalent of a digital fingerprinting of the file. For example, once you check a file with a Secure Hash Algorithm (SHA-1) hashing utility capable of generating this SHA-1 value (the digital fingerprint), that will be a fixed-length unique identifier for that file. The SHA-1 is called secure because it is computationally infeasible for two files with different content to have the same SHA-1 hash value. Law Enforcement can search the P2P networks to locate individuals sharing previously identified child exploitation material in the same way a user searches this network. When a user on the P2P network offers a file to trade, the P2P software used by law enforcement calculates a "hash value" of the file using a SHA-1 hash. A person may copy a file and rename it but if it is an exact copy, regardless of the name of the file, it will have the same hash value.

14. Most P2P programs allow users to designate specific folder(s) as "shared" folders. Any files contained in those specific folders are then made available for download by other users on the same P2P network. P2P software users typically do not "share" all of the files on their hard drive.

15. The BitTorrent network is a very popular and publically available P2P file-sharing network. Most computers that are part of this network are referred to as "peers" or "clients," hereafter referred to as a peer. A peer can download files from other peers simultaneously, and provide these files to other peers.

16. The BitTorrent network can be accessed by computers via many different client (software) programs, such as the "BitTorrent" program, the "µTorrent" program, the "BitLord" program, and the "Vuze" program, to name a few. These client programs are publicly available, typically free, and can be downloaded from the Internet.

17. During the query and/or downloading process from a suspect BitTorrent network client, certain information may be exchanged between an investigator's BitTorrent client program and the suspect client program they are querying and/or downloading a file from. This information includes 1) the suspect client's IP address; 2) a confirmation from the suspect client that they have pieces of the file(s) being requested, in whole or in part, and that the pieces of the file(s) are being reported as shared from the suspect client program; and 3) the BitTorrent network client program and version being utilized by the suspect computer. Law enforcement has the ability to log this information.

18. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address is unique to a particular computer during a specific online session. The IP address provides a unique "location," or address, as to each computer, making it possible for data to be transferred between computers.

19. The computer running P2P software has an IP address assigned to it while it is connected to the Internet. Investigators are able to see the IP address of any computer system sharing files. Investigators can then search public records that are available on the Internet to

determine the specific Internet Service Provider (ISP) who has assigned that IP address to that computer. ISPs maintain logs and records which reflect the specific IP addresses it assigned to specific computers that connect to the Internet through that ISP at any given moment. Based upon the IP address assigned to the computer sharing files, subscriber information then can be obtained from the ISP which contains identifying information of the individual to whom the account is registered.

20. The computers that are linked together to form the P2P network are located throughout the world; therefore, the P2P network operates in interstate and foreign commerce. A person who includes child pornography files in his/her "shared" folder is hosting child pornography and therefore is promoting, presenting, and potentially distributing child pornography. A person who hosts child pornography is in violation of Title 18, United States Code, Section 2252 in that he/she is promoting and presenting child pornography in interstate and foreign commerce by means of a computer.

Probable Cause

21. On Tuesday, April 17, 2018, I was conducting an online investigation on the BitTorrent network for offenders sharing child pornography. An investigation was initiated for a device at IP address 24.117.229.133 because it was associated with several torrents that had at least one file which had been identified as being a file of investigative interest to child pornography investigations. Using a computer running investigative BitTorrent software, a direct connection was made to the device at IP address 24.117.229.133, hereinafter referred to as "Suspect Device". The Suspect Device reported it was using BitTorrent client software - BL24532 BitLord 2.4.5.

22. Between April 17, 2018 and April 25, 2018, through the use of investigative BitTorrent software, I completely downloaded a total of 2,304 files directly from IP Address 24.117.229.133. Some of the downloaded files were padding files, which are related to the torrent file and did not actually contain any images or videos. I reviewed the downloaded files and found that 1,282 files depicted child pornography. Many of the files that were not padding files or child pornography files could be classified as child erotica. Of the files that depicted child pornography, 1,275 were image files and 7 were video files. Included in the some of the downloaded child pornography files were some that depicted bestiality and some that depicted bondage. In some cases attempts were made at downloading files from the same torrent on more than one occasion. Attempts were made at downloading files that were associated with 10 different torrents.

23. Below are examples of some of the child pornography files downloaded from IP address 24.117.229.133, listed by filename:

a. (Pthc) 11Yo Sara Loves To Suck Cock (4 Parts Combined By H 12-2008).avi:

This is a video file that depicts a young minor female performing oral sex on an adult male's penis.

b. IMG_0383.jpg: This is an image file that depicts an adult male having vaginal sex with a minor female who appears to be under 10 years of age.

24. An online query of the IP address 24.117.229.133 through the American Registry for Internet Numbers identified the IP address to be registered to Cable One. An administrative subpoena was issued to Cable One requesting subscriber information for the user of this IP address during the time the files were downloaded between April 17, 2018 and April 25, 2018.

The resulting information from Cable One revealed the subscriber was Patricia Sheats with an address of 116 North Rogers Avenue, Bartlesville, Oklahoma.

25. On September 09, 2019 I travelled to 116 North Rogers Avenue in Bartlesville, Oklahoma with FBI Task Force Officers to investigate the above described BitTorrent activity. Agents (who did not have a search warrant) knocked on the door of the home upon arrival and identified themselves as law enforcement, requesting someone to answer the door. A few moments later a male who identified himself as Patrick Aaron Sheats answered the rear door of the home. Agents advised Sheats of the nature of their visit and subsequently interviewed Sheats outside. Through the course of the interview Sheats provided his consent for Agents to search multiple electronic Devices, which were inside his home. One such device was a Dell All-In-One computer having serial number FLQB022. This computer was searched during the interview of Sheats through the use of a program called OS Triage. The OS Triage program identified child pornography files and related activity on the Dell All-In-One computer. Sheats initially denied being involved in child pornography but later admitted to his activities. Sheats described that he would search for child pornography torrents on the internet and then download them using BitTorrent. Sheats claimed to have first seen child pornography about 2 years prior and denied downloading any child pornography in the past 5 or 6 months. Sheats admitted that the child pornography activity detected by Agents in April of 2018 would have been committed by him.

26. During the course of the interview Sheats provided consent to search the following devices that he provided to Agents from his home:

- Dell All-In-One computer, serial number FLQB022
- Dell Laptop computer, serial number 9R923S1

- Western Digital hard drive, serial number WCC1S7961393
- Seagate hard drive, serial number W1F4FBQR
- SanDisk solid state drive, serial number 124675402476
- The Devices were returned to the Tulsa Resident Agency of the FBI and entered into evidence. The devices have been transferred to the FBI's Oklahoma City Division headquarters office where an examination of the devices will be completed.

27. Below are descriptions of some of the child pornography files located during the search of the Dell All-In-One computer using the OS Triage program on September 09, 2019:

- a. pthc ohdaddy1-7 5yo fucked by daddy (very excellent).avi: This is a video file that depicts an adult male having vaginal sex with a minor girl who appears to be under 10 years of age.
- b. russian kids 2-bambina(3).avi: This is a video file that depicts a minor female who appears not to have yet reached the age of puberty performing oral sex on an adult male.
- c. russian kids 2-bambina(3).avi: This is a video file that depicts a minor female who appears to be under the age of 10 and an adult male. The video shows the minor female performing oral sex on the adult male and the adult male having vaginal sex with the minor female.

FORENSIC ANALYSIS

28. Based on my knowledge, training, and experience, I know that electronic devices, such as a computer and hard drive can store information for long periods of time. Similarly, things that have been viewed via the internet and various software applications are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools. I know that digital files, such as child pornography pictures and videos, can be transferred from one device to another; copies can also be stored simultaneously on multiple devices. Thus, I'm requesting to search all of the Devices, not just the Dell All-In-One computer

described above. I know based on my training and experience that child pornography collectors such as Sheats often store their collections on multiple devices.

29. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited.
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a device is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual

information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.


30. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

31. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

Conclusion

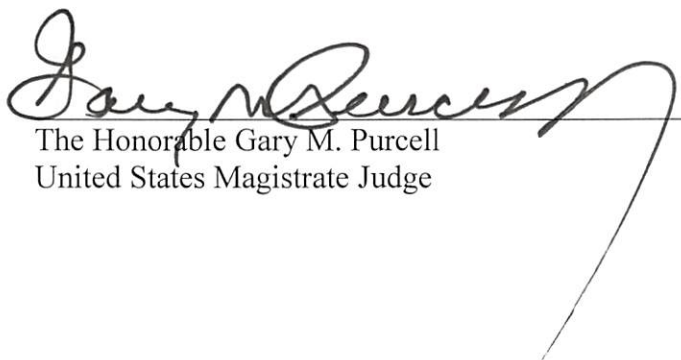
32. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,



Richard Whisman
Special Agent
Federal Bureau of Investigation

SUBSCRIBED and SWORN to before me on the 8th day of November, 2019



The Honorable Gary M. Purcell
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

The property items to be searched are: a Dell All-In-One computer with serial number FLQB022, a Dell Laptop computer with serial number 9R923S1, a Western Digital hard drive with serial number WCC1S7961393, a Seagate hard drive with serial number W1F4FBQR, and a SanDisk solid state drive with serial number 124675402476, which are currently in the possession of the Federal Bureau of Investigation in Oklahoma City, Oklahoma.

fw
4mb

ATTACHMENT B

Particular Things to be seized

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Section 2252, for distributing and accessing, and attempting to access, with intent to view child pornography:

1. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;
 - d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
 - e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
 - f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
 - g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
 - h. evidence of the times the COMPUTER was used;

mw
gwb

- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
- m. contextual information necessary to understand the evidence described in this attachment.
- n. Child pornography and child erotica, and evidence of accessing the same.

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

A handwritten signature in blue ink, appearing to be "J. Smith", is located in the bottom right corner of the page.